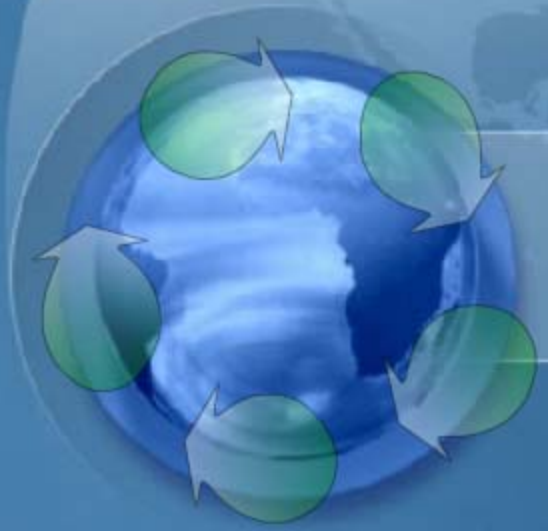
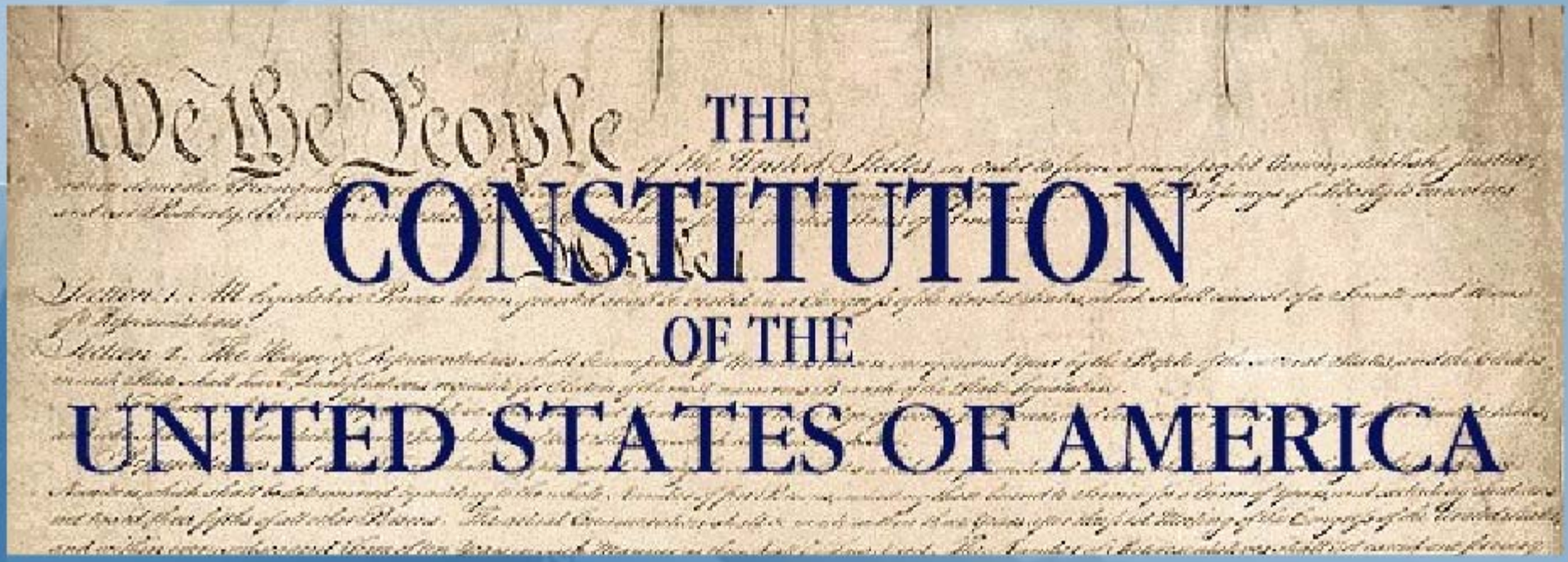
Office of Science



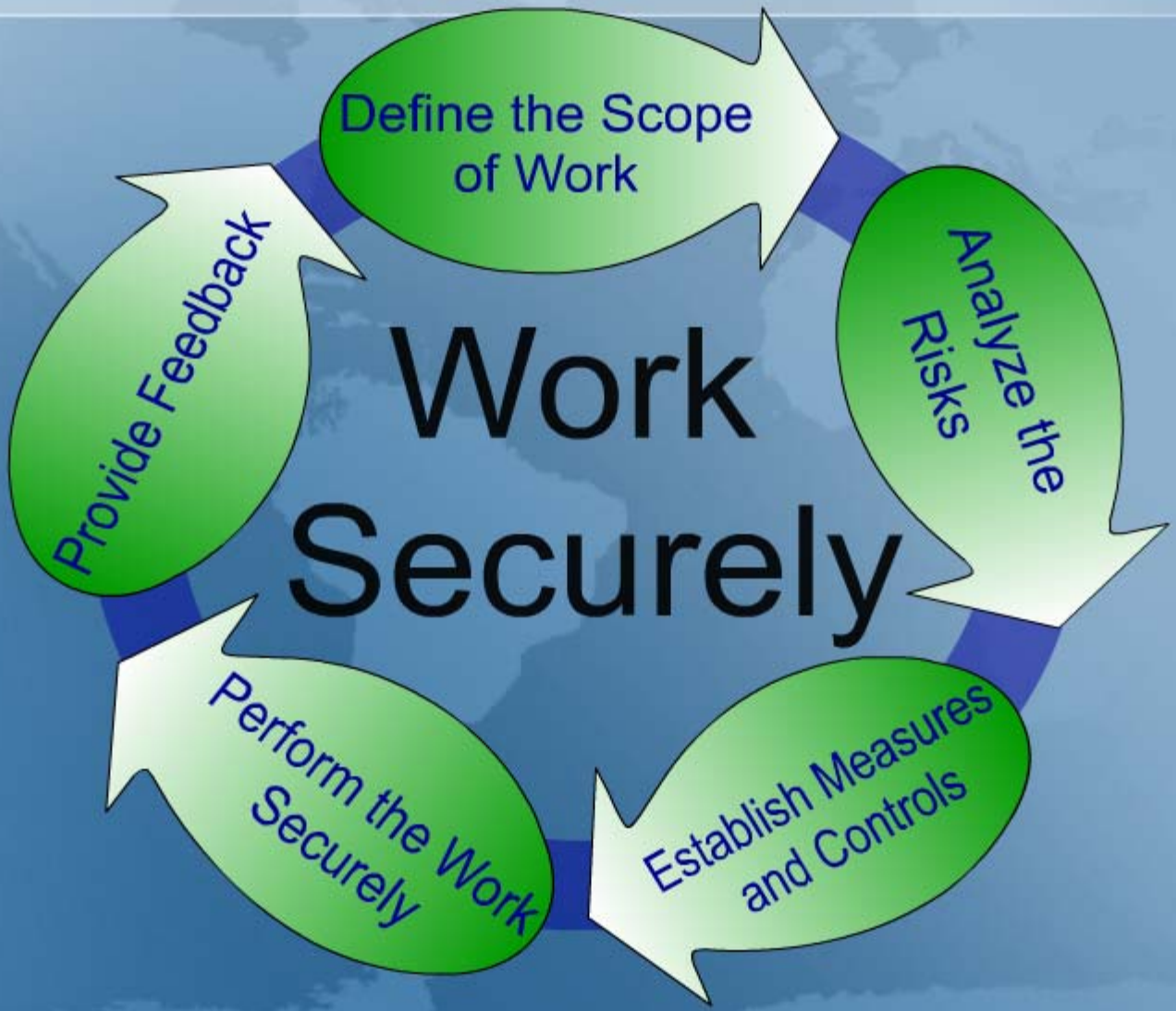
2002 Annual Security Briefing

Presentation by
Security Management Staff



"We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty, to ourselves and our Posterity, do ordain and establish this constitution for the United States of America."

ISSM


Define the Scope of Work
Analyze the Risks
Establish Measures and Controls
Perform the Work Securely
Provide Feedback
Work Securely

Integrated Safeguards and Security Management (ISSM)

Dr. Raymond L. Orbach

"I believe that there is no conflict between the goals of great science and good security. We must and will do both. And the way to accomplish both is through the integration of science and security, in much the same way we are integrating science and safety. Specifically, we must ensure that ultimately, each individual scientist understands the security issues at stake, and incorporates these into the way they conduct their work."

National Academy of Science, May 13, 2002.

Drivers of Change

- **SC Restructuring**
- **Homeland Security**
- **Commission on Science and Security - Hamre Report**
- **Government Information Security Reform Act Report**

We the People

Table of Contents

We the People

ISSM Starts With YOU

Whether at work, on travel or working remotely.

- Badges
- Remote Computer Access
- Conversations
- Official Use Only (OUO) - "taking work home"

ISSM Starts With YOU

Working Remotely

Should be done cognizant of the possible security risks. You are responsible to determine Official Use Only (OUO) and to know what OUO is.

ISSM Starts With YOU

Official Use Only

Information to be withheld Must Meet Two Criteria

- **First Criterion**:
  - Sensitivity: Must be sufficiently sensitive that it should not be publicly released if requested under FOIA
- **Second Criterion**:
  - 9 Exemptions: Must fall within the scope of one of the nine exemptions

ISSM Starts With YOU

Official Use Only

Nine Exemptions:

1. National Security Information
2. Internal Agency Practices
3. Information required to be withheld by statute
4. Commercial/Propriety
5. Deliberative Process
6. Personal
7. Investigatory
8. Banks
9. Wells

http://www.usdoj.gov/oip/foi-upd.htm

ISSM Starts With YOU

Official Use Only

Authorities – You are the responsible individual acting in an official capacity who will determine and mark a document as OUO.

ISSM at Work

Entry procedures:

Gates (vehicle inspections)

We the People

ISSM at Work

Physical Security

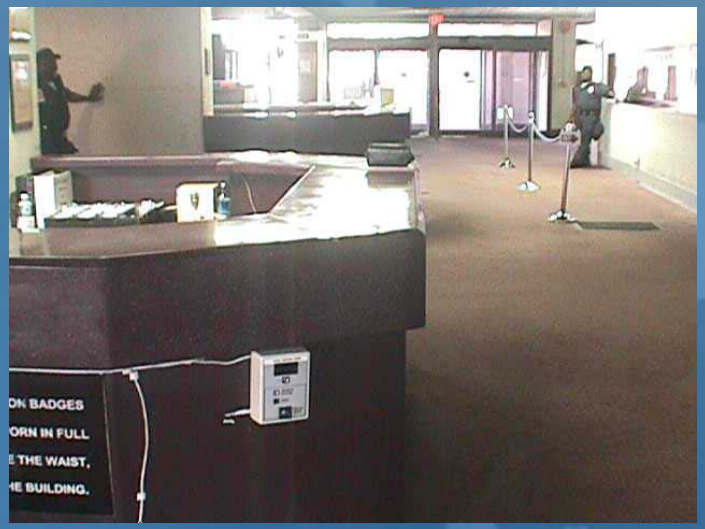
- ***Prohibited Items*** (installation of personal software on government systems, Firearms, Explosive Materials, Controlled Substances, etc).

- ***Prohibited Items in Security Areas*** (Radio frequency transmitting equipment, Privately owned electronic equipment w/ a data port, Privately owned computers and associated media, Palm Pilots and Black Berries).

ISSM at Work

Physical Security

Protective Forces (Access Control, Badges, Random Inspections and Property Passes).



ISSM at Work

"GARTH"

Canine Explosive Detection Team

- Assist with truck and package inspections
- Routine patrols of exterior portions of the building
- In order to ensure that the dog focuses on detection activities, DOE employees are requested to **avoid any contact with the animal** without prior acknowledgment and approval from the handler

ISSM at Work

Security Conditions (SECONs)

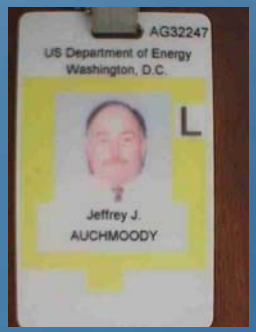
Secon 3

REAT DESCRIPTION	DOE SECON LEVEL	HSAS COLOR	HSAS* THREAT DESCRIPTION
Negligible: Normal Security Operations	5	Green	**Low**: Low risk of terrorist attack
Low: Increased general threat of malevolent or terrorist activities	4	Blue	**Guarded**: General risk of terrorist attack
Medium: Increased and more predictable threat of malevolent or terrorist activities	3	Yellow	**Elevated**: Significant risk of terrorist attack
High: An incident occurs or intelligence is received indicating that some form of malevolent or terrorist action is imminent	2	Orange	**High**: High risk of terrorist attack
Critical: A malevolent or terrorist attack has occurred or when intelligence has been received that a terrorist or malevolent attack against a specific location or person is likely.	1	Red	**Severe**: Severe risk of terrorist attack

* HSAS – Homeland Security Advisory System

ISSM at Work

Badges



- ***Top Secret*** – "Q" (RD, FRD, NSI)
- ***Secret*** – "L" (FRD/NSI)
- ***Confidential*** – "L" (RD)
- ***Building Access* ONLY**– "N" Only

❖ ***Contact the Lab you need to visit in advance for site specific access procedures.***

We the People

ISSM at Work

Badges

- Your badge should be worn at **all times** while at work.
- If your badge is lost/stolen, report it to the Security Management Staff **immediately**

ISSM at Work

Contractor Badges

Contractor Badges expire on the date given as the contract expiration date/end date of detail on the original badge request.

The sponsor should initiate updated badge cards (TYPED or PRINTED legibly) as soon as a contract or detail has been extended or renewed.

Please be aware that the DOE sponsor is not the person that should sign pre-employment checks.

Do not assume US citizenship.

Remember to Plan Ahead

Contact: Sabeena Rangwala:

F-242/3-4681

ISSM at Work

Security Updates

Effective immediately, the following inspection procedures will be enforced at DOE Headquarters facilities:

- Box Inspection - All boxes will be inspected when being brought into or taken out of a facility.
- Cell Phones - Property passes for cell phones are not required.

ISSM Starts With YOU

Cyber Security

- Consider ISSM in cyber security.
- You protect information and systems against unauthorized remote access, modification of information, and information theft.

ISSM Starts With YOU

Cyber Security

- **Anti-virus** software can prevent the spread of known viruses, Trojans and backdoors.
- Opening **attachments** from people that you do not know – or that have strange messages can contain bad payloads.
- Do Not Use the same password for home and work, use **strong passwords**, and do not give others access to your work accounts.
- Downloading unapproved software and applications
- Lack of Backups

(Handout) http://www.ftc.gov/bcp/conline/edcams/infosecurity/

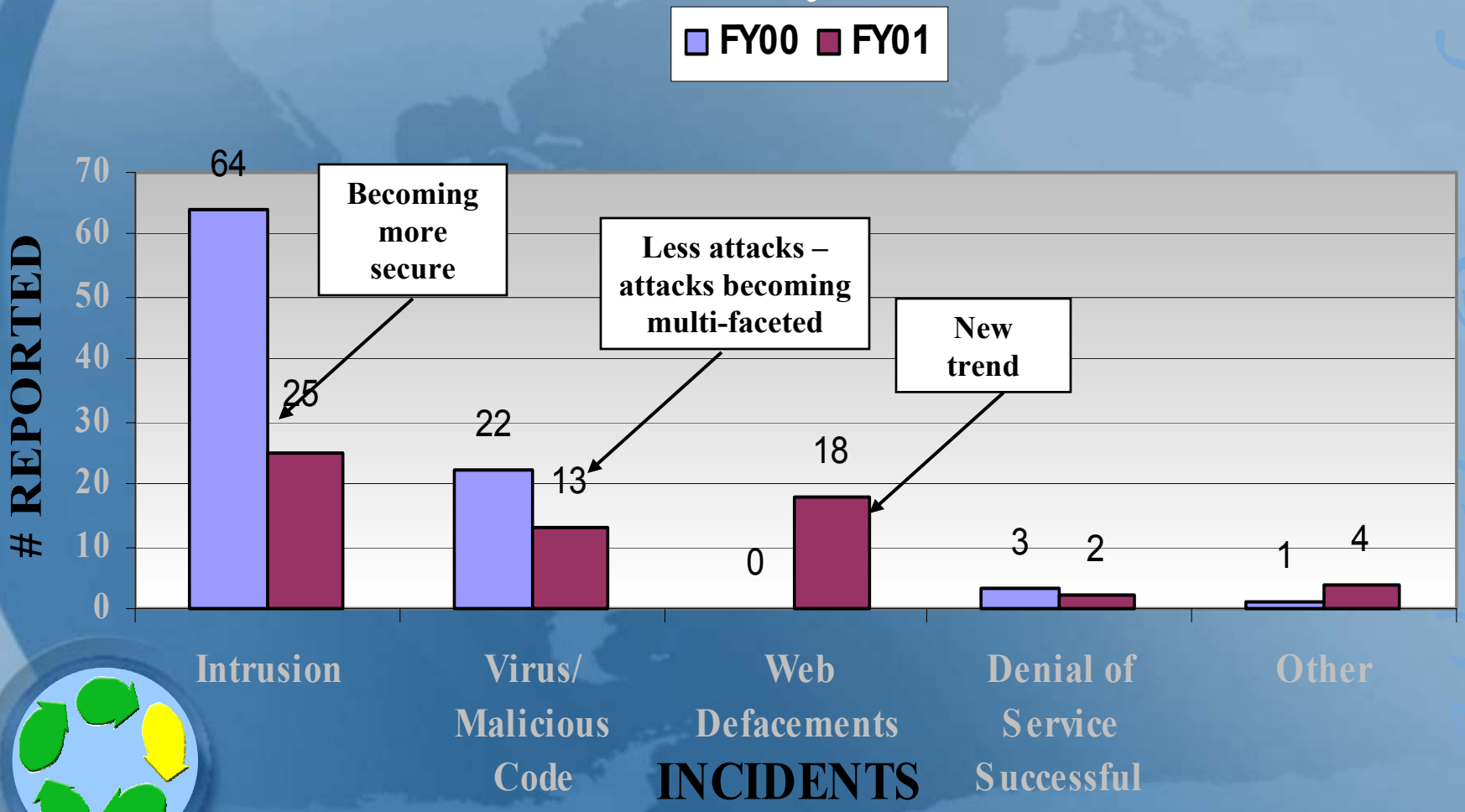
ISSM at the Desktop

Unsolicited E-Mails

If anyone receives repetitive email scams, repetitive unwanted solicitation, threats, or any offensive material forward it SCSC and cc Susan Lister.

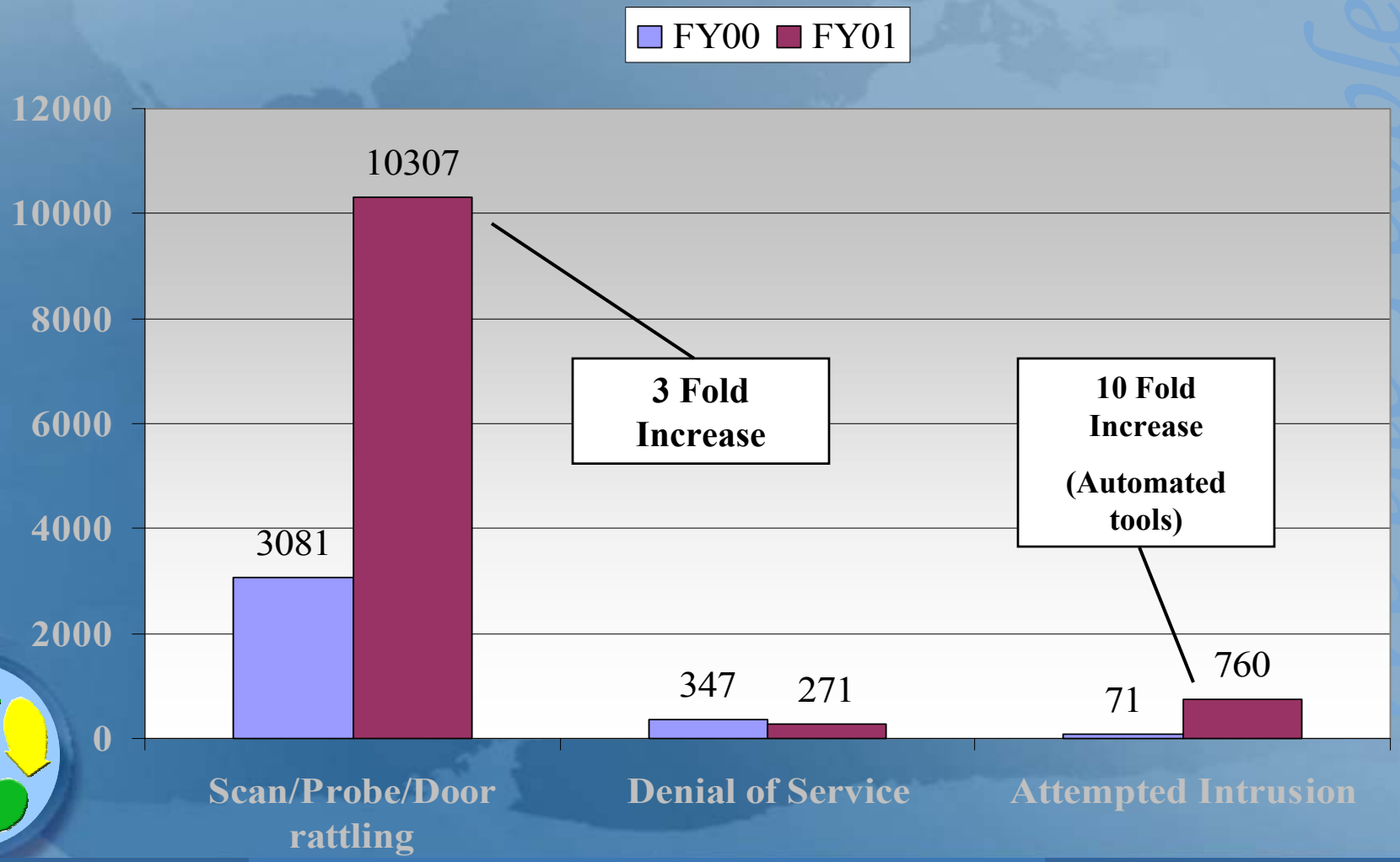
ISSM at the Desktop

SC Site-wide Cyber Incidents



ISSM at the Desktop

SC Anomalous Cyber Activity



ISSM at the Desktop

Questions Regarding Cyber Security?

Please Contact:

Susan Lister (HQ and Sites) at 3-3462,

SCSC (SC-65) at 3-5313,

ESNET (SC-31) at 3-0071

We the People

ISSM at Work

Working with OUO or Classified Information

Information Security ensures that materials and documents, that may contain OUO or Classified information are properly reviewed for content and protected from unauthorized disclosure, and ultimately destroyed in an appropriate manner.

We the People

ISSM at Work

Access to Classified Information

- Must have a NEED TO KNOW
- Proper Security Clearance Required

ISSM at Work
Classification Categories

Types of Classified Matter and Classification Levels			
Type of DOE Access Authorization	**Restricted Data** (Design or manufacture of weapons, production of SNM or use in Emergency)	**Formerly Restricted Data** (Utilization of Nuclear Weapons)	**National Security Information** (Information pertaining to National Security)
Q – Permits access to these levels of classified matter if there is **need to know**	**Top Secret** **Secret** **Confidential**	**Top Secret** **Secret** **Confidential**	**Top Secret** **Secret** **Confidential**
L – Permits access to these levels of classified matter if there is **need to know**	**Confidential**	**Secret** **Confidential**	**Secret** **Confidential**

ISSM at Work

Classified Conferences and Discussions

Classified conferences and discussions, or classified document storage & review can ONLY be held in approved Security areas at Germantown and Forrestal. The SC Security Area is located in:

GTN G-222

FORS 3H-017

Contact:

Mark Thornock (3-2995)

Sabeena Rangwala (3-4681)

ISSM at Work

Proper Handling of Classified and OUO Information

- Transfer in sealed, opaque envelopes
- Use of U.S. Postal Service is authorized
- OUO Info: Use of proper electronic transmission

***If you need to receive, send or process Classified contact the SMS first for proper addresses/packaging etc .**

ISSM at Work

New OUO Disposal Method

- The new option on destruction of OUO trash is to purchase shredders from the supply store.
- Cost is approximately $225 per *cross cut shredder (the type recommended by Office of Security) and available within 4 weeks if supply store doesn't have any in stock.

(*Crosscut shredders can handle staples)

ISSM at Work

The Old OUO Disposal Method

Remove paper clips, staples and metal/plastic fasteners; put in a <u>brown bag</u>

The Bag MUST have the following information in <u>Black marker</u> *(NOT a regular tip pen)* on it:

- Full Name
- Last five digits of your phone number
- Routing Symbol/ Room No.

Trash will not be accepted without the listed information.

Call security at 3-2403 to have them open room R-002 for trash disposal. At Forrestal take your trash down to room GA-085 M,W,F, from 3-4 p.m.

Note: Each bag must weigh no more than <u>10 pounds</u> or it <u>will not be accepted.</u>

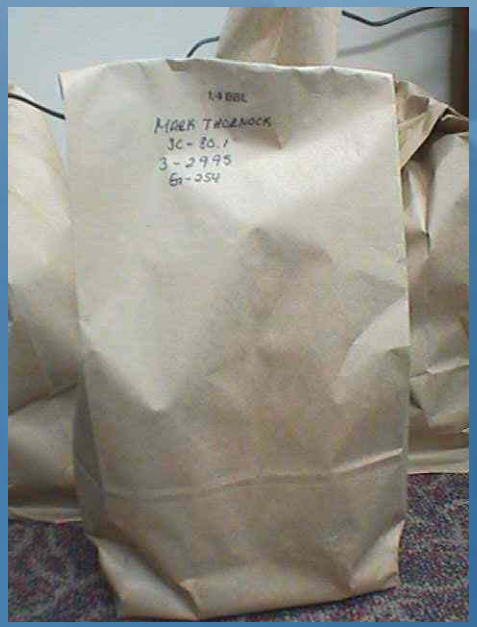
ISSM at Work

Classified Disposal

- Classified Information for disposal must be put in a **red/white candy-striped burn bag.**
- Write the same information as is required for OUO burn bags on the outside of the bag.

ISSM at Work

Operation Clean Sweep

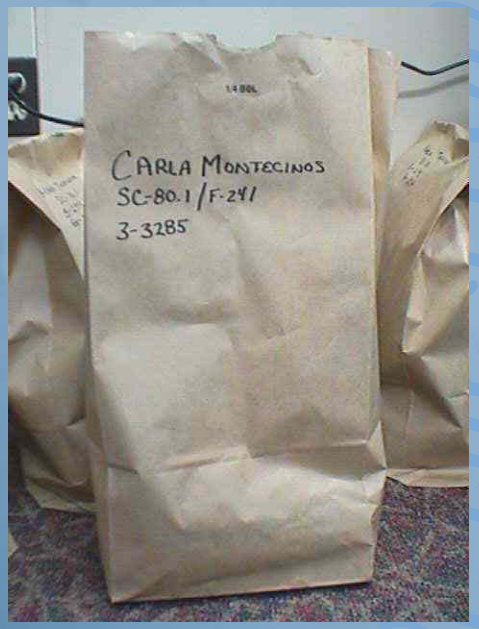


FORS – OCT 28th, 2002

3:00 p.m. – 4:00 p.m.

GTN – OCT 31st, 2002

Afternoon



ISSM at Work

Operation Clean Sweep

Include Electronic Files

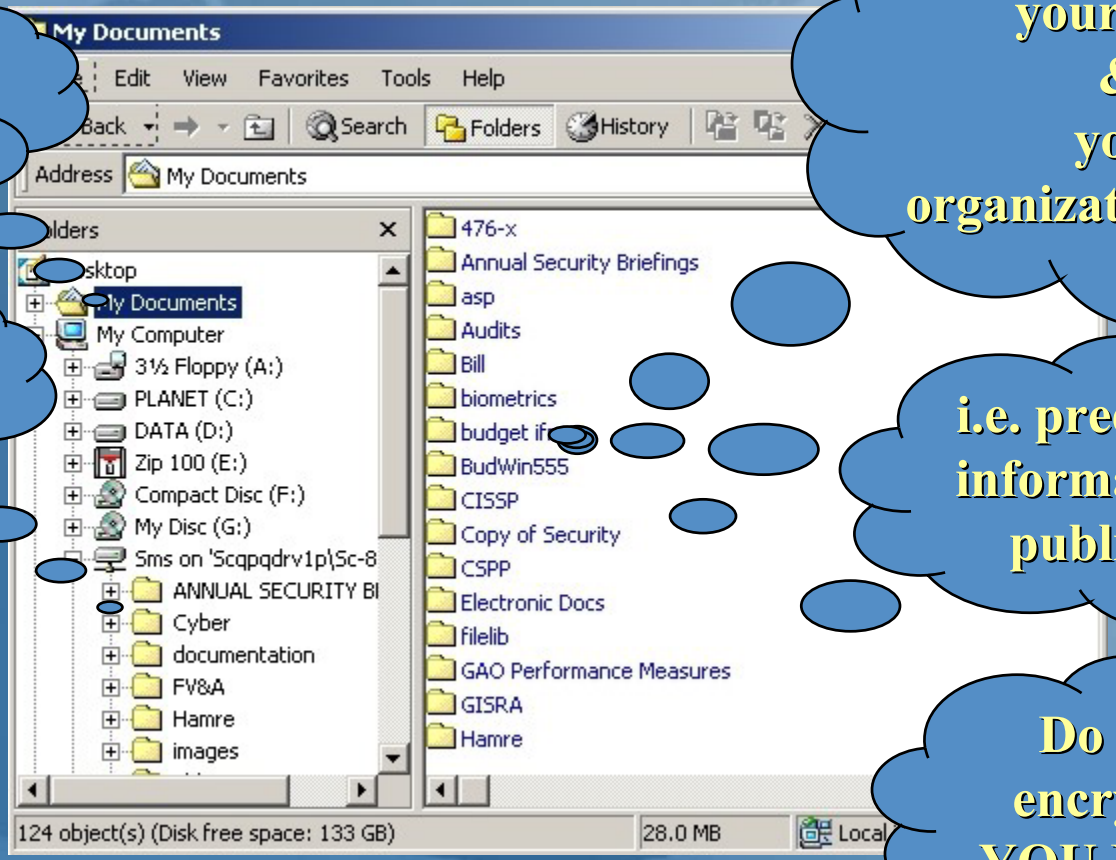
My Documents

Organize or delete your files & your organization's files

Network Drives

i.e. predecisional information on a public drive

Do I need encryption? YOU DECIDE



ISSM at Work

Any Emergency

DIAL 166

Report the emergency to
Protective Force

Health Unit Numbers:

Forrestal	6-9765
Germantown	3-4275

We the People

ISSM at Work

In CASE of a BOMB THREAT

Telephone vs. Voice Mail

Telephone:

1) **While listening** — **DIAL Flash then 11** (conference #3 on some phones).

1) **Lay Phone down and DIAL 166** (from different phone).

2) **Fill out Checklist** (contact Mark Thornock).

Voice Mail:

1) **Hang up** (do not save, archive, transfer).

2) **Dial 166** (to file a report).

3) **Checklist** (fill out Bomb Threat Check List and contact Mark Thornock from the SMS).

ISSM on Foreign Travel

The risk of becoming an intelligence target increases greatly during foreign travel. As an American government official, scientist, or business traveler with access to useful information, you can become the target of a foreign intelligence or security service at ANYTIME in ANY country.

Assume that you are being observed and overheard at all times while on official travel!
(This includes cell phones, laptops, blackberries.)

ISSM on Foreign Travel

Official Foreign Travel

All DOE employees, federal or contractor, traveling to a foreign country on *official government business:*

- WILL fill-out a request for approval of Foreign Travel on the Foreign Travel Management System website (https://ftms.doe.gov)
- You can access a printed form, to later enter into the system from the site
- Counterintelligence may brief you before you leave the country and debrief you when you come back.
- If you have any questions contact Nancy McDonough 3-6050

ISSM on Foreign Travel

Unofficial Foreign Travel

If you HOLD or have HELD, within the Last Five Years a DOE Q or L Security Clearance and visit:

Sensitive Countries: DOE Order 551.1A REQUIRES you to fill out DOE form F1512.1 thirty days prior to travel and provide it to Nancy McDonough 3-6050 in room F-237

Non-sensitive Countries:

For your safety contact HSO-Mark Thornock 3-2995 in room G-241 for security information - http://www.state.gov

ISSM at Work

Visitors

All Visitors must have a point of contact, sign in and have an escort during security hours or in security areas irrespective of citizenship.

Be Aware: If any of the visitors are foreign nationals then their information must be processed through the FACTS System.

ISSM at Work

Foreign Visits & Assignments (FV&A)

As soon as you know of a foreign visit please contact *Carla Montecinos* at 3-3285 or stop by her office in room F-241.

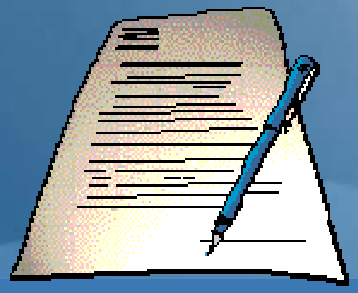
- If from a *Non-Sensitive Country*: short form is to be used and submitted 7 days prior to the visit.
- If from a *Sensitive/Terrorist Supporting Country*: long form is to be used and submitted 30 days prior to the visit.

ISSM at Work

SC Delegation

- Dr. Orbach delegated approval authority for Headquarters Office of Science foreign visits and assignments to each Associate/Office Director.

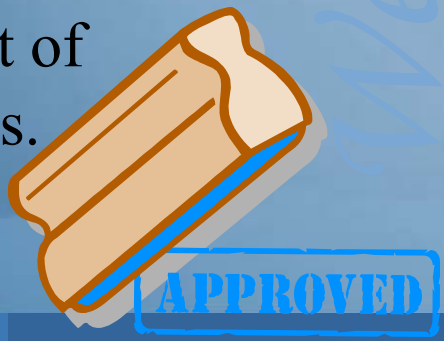
- In the absence of the Associate/Office Director, or for visits by foreign nationals to the SC front office, Dr. Harold Jaffe will handle the approval (*May 23, 2002* Memorandum From: *Raymond L. Orbach* Director Office of Science).



ISSM at Work

Foreign Visitors

- Foreign nationals cannot have access to cyber systems without prior approval from an appropriate Associate Director/Office Directors, and a documented security plan.
  - Identify the specific cyber system(s) to which access is granted and the anticipated time period of the access, and
  - Must be based on a documented assessment of risks and an identification of access controls.



ISSM at Work

Host Reports

Host Reports are due to Carla within 15 days of a visit. Host Report Forms are available from Carla Montecinos.

ISSM at Work

J-1 Visa Waivers

The **HOST** and **SPONSOR** must be familiar with the J-1 Visa waiver checklist. (Handout)

If you have any questions or want to talk more about the program please stop by our office (F-241/242) or call ***Carla Montecinos*** at **3-3285.**

We the People

COUNTERINTELLIGENCE

Analyze Risk

ISSM at Home, Travel and Work

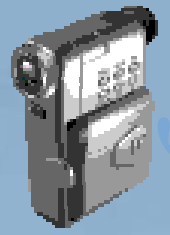
Counterterrorism

Terrorist Threats

- Success in the war against terrorism is supported by **individual awareness**. By using the following threat indicators and maintaining heightened awareness you can actively help protect your family, friends, and co-workers from terrorist activities.

ISSM at Home, Travel and Work

Counterterrorism



Indicators

- Personnel observed near facility using/carrying video camera or other observation equipment e.g., night vision devices
- Personnel observed parking, standing or loitering over several days with no apparent reasonable explanation
- Unidentified vehicles e.g., no site access sticker

ISSM at Home, Travel and Work

Counterterrorism

Indicators

- Unusual questioning about the facility or personal information
- Abandoned parcels or suitcases
- Low-flying aircraft, possibly observing the area
- Any activity considered suspicious to you

ISSM at Home, Travel and Work

Visits to SC Facilities

Things to look for:

- "Wandering" visitors who act offended when confronted
- Questions outside the scope of the visit
- Hidden agenda: visit related to Project X, but questions and discussion focus on Project Y

ISSM at Home, Travel and Work

Other Indicators of – Suspicious Activity

- Indicators of critical interest include:
  - Attempts to obtain information without a need to know (usually repeated or outside the scope of their job)
  - Unexplained/excessive use of copiers (outside normal routine)
  - Living beyond one's means or sudden reduction of large debts
  - Unusual travel patterns (unexplained trips of short duration to same locale)

ISSM at Home, Travel and Work

Presidential Decision Directives (PDD)

The following two PDDs set the guidelines for the Counterintelligence Program:

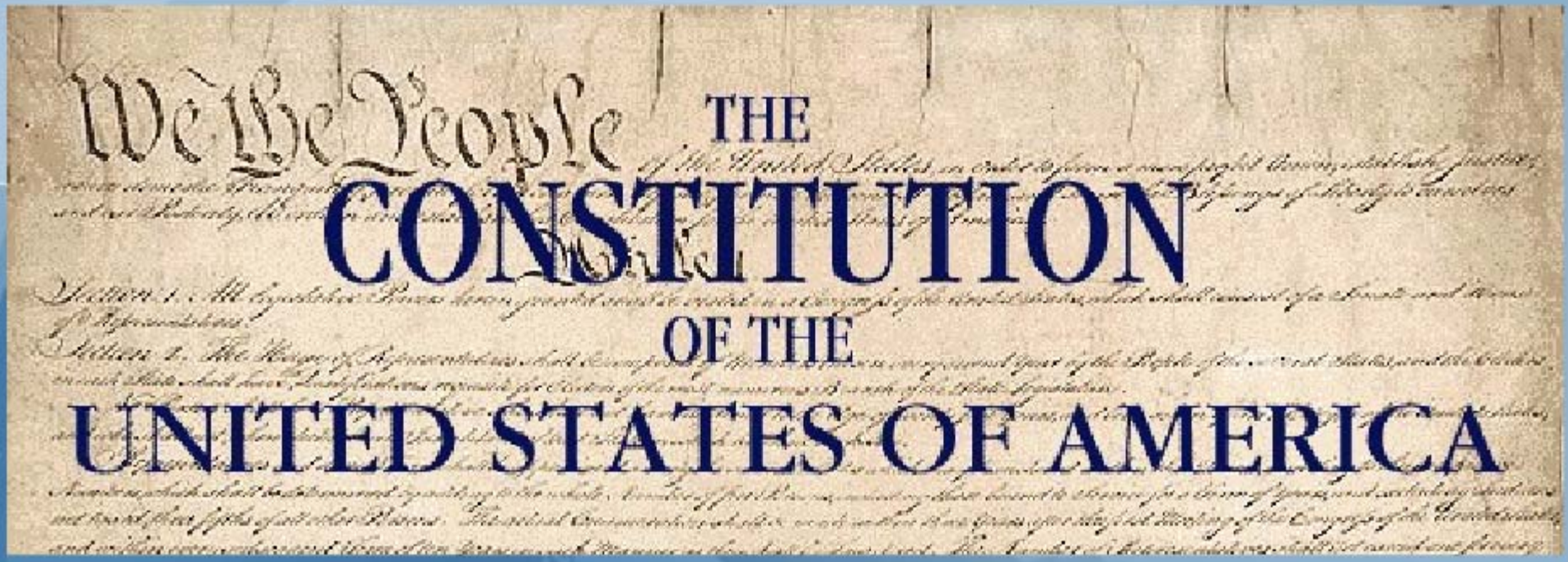
- PDD-12 (*8/93*) Security Awareness & Reporting of Foreign Contacts.
  - Requires that government employees report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which illegal or unauthorized access is sought to classified or otherwise sensitive information or the employee is concerned that he/she may be the target of exploitation by a foreign entity.
- PDD-61 (*2/98*) Energy Department Counterintelligence.
  - The Implementation of PDD-61 has included changing the screening and the approval process for foreign scientists to DOE labs, making the laboratory Directors directly accountable for foreign visits, and instituting more extensive security reviews-including the use of polygraphs.

ISSM at Home, Travel and Work

Counterintelligence

If you think you have any concerns, then you should contact:

Mark Thornock (SC) at 3-2995
or
Lee Luna (CN) at 6-8751
or
Robert Thompson (CN) at 3-0434



"We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty, to ourselves and our Posterity, do ordain and establish this constitution for the United States of America."

Questions?

http://www.science.doe.gov/SC-80/security/

Don’t forget to fill out the evaluation